**به نام خدا**

استاد : یوسفی

دانشجو : میر امیرحسین میرمحمدی آتشگاه و زهرا اصغریان

موضوع : امنیت سیستم های مدیریت اطلاعات

**مقدمه**

هر سیستم برای ادامه ی حیات و زندگی خود نیازمند کسب اطلاعات گوناگون و همچنین حفاظت از اطلاعات و اسرار خود می باشد و مبحث کسب اخبار و اطلاعات از زمانهای قدیم مرسوم بوده و بعضا دستیابی یا نشر اطلاعات یک سیستم باعث نابودی آن سیستم گشته . امروزه با توجه به اینکه اطلاعات به عنوان یک ابزار تجاری و رقابتی و سرمایه ای سودآور مطرح گردیده بسیاری از سازمانها به دنبال ایجاد سیستمهای امنیتی برای جلوگیری از درز اطلاعاتشان به بیرون می باشند تا بتوانند کل مجموعه خود را حفظ کنند در این راستا ایجاد یک سیستم امنیتی قوی می تواند برای حفظ امنیت اطلاعات هر سازمان موثر باشد سیستمی که بر اساس نیازهای سازمان و میزان اهمیت اطلاعات در آن طراحی شده باشد و حفاظی باشد جهت تامین سرمایه های اطلاعاتی . سیستم مدیریت امنیت اطلاعات ( ISMS )ابزاری مناسب است در جهت طراحی و کنترل امنیت اطلاعات.

**تعریف**

ISMS مخفف "Information Security Management System" است. ISMS یک سیستم مدیریت یکپارچه است که شامل مجموعه ای از کنترل های امنیتی است که از محرمانه بودن، در دسترس بودن و یکپارچگی دارایی ها در برابر تهدیدها و آسیب پذیری ها محافظت می کند. سیستم مدیریت امنیت اطلاعات (ISMS) چارچوبی از سیاست‌ها و کنترل‌هایی است که امنیت و خطرات را به طور سیستماتیک و در کل امنیت اطلاعات سازمان شما مدیریت می‌کند. این کنترل های امنیتی می توانند از استانداردهای امنیتی رایج پیروی کنند یا بیشتر بر صنعت شما متمرکز شوند.

با طراحی ، پیاده سازی ، مدیریت و نگهداری یک ISMS ، یک سازمان می تواند از اطلاعات محرمانه ، شخصی و حساس خود در برابر نشت ، آسیب ، تخریب یا قرار گرفتن در معرض عناصر مضر محافظت کند. ISMS شامل چگونگی شناسایی افراد، سیاست ها، کنترل ها، سپس رسیدگی به فرصت ها و تهدیدهای حول اطلاعات ارزشمند و دارایی های مرتبط است.

## سازگاری سیستم مدیریت امنیت اطلاعات (ISMS) با سایر سیستم های مدیریتی

ISMS از استاندارد خانواده بزرگ استاندارد ISO 27000 پیروی می کند. در واقع این استاندارد راهنمای جامعی برای پیاده سازی ISMS است. در راستای پشتیبانی از پیاده سازی و اجرای یکپارچه و سازگار با استانداردهای مدیریتی مرتبط، ISMS با سایر سیستم های مدیریتی همچون ISO 9001 و ISO 14001 تطبیق داده شده است. بنابراین یک سیستم مدیریتی که به گونه ای مناسب طراحی شده باشد، می تواند الزامات تمامی این استانداردها را برآورده سازد. و ISMS این توانایی را در خود ایجاد کرده است.

استاندارد ISO/IEC 27001 زمینه مناسبی را برای طراحی و استقرار سیستم مدیریت امنیت اطلاعات و ارزیابی آن در سازمان ها و بهره گیری از منافع این رویکرد، فراهم آورده است. سیستم مدیریت برحسب امنیت اطلاعات، به یک سازمان این امکان را می دهد تا موارد زیر را ایجاد نماید:

- * رضایت نیازمندی های امنیتی مشتریان و سایر ذینفعان

- * بهبود طرح ها و فعالیت های سازمان
- * تأمین اهداف امنیت اطلاعات سازمان
- * تطابق با آیین نامه ها و قوانین و مقررات مربوط به کار

**خطرهای تهدید کننده ی سیستم اطلاعاتی**

خطرهای تهدید کننده ی امنیت اطلاعات به دو دسته ی عمدی و غیر عمدی تقسیم می شوند ، خطرهای عمدی خطرهایی هستند که امنیت اطلاعات سیستم را با برنامه ی قبلی و هدفی خاص مورد حمله قرار می دهند مثل خطر هکرها و خطرهای غیرعمدی خطرهایی هستند که بر اثر اشتباهات انسان و نیروی کار به سیستم وارد می شود که این نوع خطر بیشترین میزان خسارات را به سیستم اطلاعاتی وارد می کنند همچنین خطرهای ناشی از عوامل طبیعی مثل سیل ،زلزله،طوفان و... جزء تهدیدات غیر عمدی به حساب می آید .

برای اینکه در سیستم ها بتوانیم خطرهای موجود را رفع کنیم قبل از هر چیز باید به فکر ایجاد امنیت شبکه های اطلاعاتی خود باشیم این ایجاد امنیت ابتدا باید شامل اتخاذ سیاست های امنیتی باشد.مواردی که یک سازمان برای پیاده سازی یک سیستم امنیتی اعمال می کند به شرح زیر می باشد :

۱)تعیین سیاست امنیتی

۲( اعمال سیاست های مناسب

۳( بررسی بلادرنگ وضعیت امنیت اطلاعاتی بعد از اعمال سیاست امنیتی

۴)بازرسی و تست امنیت شبکه ی اطلاعاتی

۵( بهبود روش های امنیت اطلاعاتی سازمان

## چارچوب های محبوب ISMS

ISO 27001 پیشرو در امنیت اطلاعات است، اما سایر چارچوب ها نیز راهنمایی های ارزشمندی را ارائه می دهند. این چارچوب های دیگر اغلب از ISO 27001 یا سایر دستورالعمل های خاص صنعت وام گرفته می شوند.

ITIL، چارچوب مدیریت خدمات به طور گسترده پذیرفته شده، دارای یک جزء اختصاصی به نام مدیریت امنیت اطلاعات (ISM) است. هدف ISM تراز کردن فناوری اطلاعات و امنیت کسب و کار است تا اطمینان حاصل شود که InfoSec به طور مؤثر در همه فعالیت ها مدیریت می شود.

COBIT، یکی دیگر از چارچوب‌های متمرکز بر فناوری اطلاعات، زمان قابل توجهی را صرف این موضوع می‌کند که چگونه مدیریت دارایی و مدیریت پیکربندی برای امنیت اطلاعات و همچنین تقریباً هر عملکرد دیگر ITSM (حتی آنهایی که با InfoSec مرتبط نیستند)، اساسی هستند.

**کنترل‌های امنیتی ISMS**

همانطور که در استاندارد ISO 27001 مشخص شده است، ISMS به کنترل دامنه‌های مختلفی از امنیت اطلاعات می‌پردازد (به سازمان‌ها و افرادی که قصد پیاده‌سازی استاندارد ISMS را در بسترهای تحت کنترل خود دارند، توصیه می‌شود که متن این استاندارد را به طور کامل مطالعه کنند). استاندارد ISMS شامل دستورالعمل‌هایی‌ست که اهداف زیر را دنبال می‌کنند:

**سیاست‌های امنیت اطلاعات:**
برای کمک به ایجاد سیاست‌های امنیتی مناسب، باید جهت‌گیری درست و پشتیبانی کلی انجام شود. در این استاندارد، خط‌مشی امنیتی برای هر سازمانی منحصربه‌فرد است؛ بدین صورت که متناسب با تغییر نیازهای تجاری و امنیتی سازمان شما، طراحی می‌شود.

**مدیریت ارتباطات و عملیات:**
درنظر گرفتن احترام و حفظ سیاست‌ها و کنترل‌های امنیتی در اداره سیستم‌ها، باید در دستورکار قرار گیرد. همچنین برای انجام عملیات روزانه فناوری اطلاعات، مثل ارائه خدمات و مدیریت مشکلات، باید پیروی از سیاست‌های امنیتی IT و کنترل ISMS در دستورکار قرار گیرد

**کسب سیستم، توسعه و نگهداری سیستم‌های اطلاعاتی:**
در تمام چرخه حیات سیستم‌های IT ، مثل مراحل دستیابی، توسعه و نگهداری، باید بهترین شیوه‌های امنیتی حفظ شوند.

**کنترل دسترسی‌ها:**
با استفاده از این دستورالعمل، دسترسی‌های پرسنل مجاز محدود شده و نظارت بر ترافیک شبکه و رفتارهای غیرعادی نیز انجام می‌شود. درنظر داشته باشید که نقش‌ها و مسئولیت‌های افراد باید به درستی تعریف شده باشند و در تنظیم دسترسی به اطلاعات تجاری، لزوم دسترسی و نقش فرد درنظر گرفته شود.

**رمزنگاری:**
یکی از کنترل‌های مهم و موثر برای محافظت از اطلاعات حساس، رمزنگاری آن‌هاست. بنابراین ISMS نیز بر نحوه اجرا و مدیریت کنترل‌های رمزنگاری نظارت دارد.

**روابط تامین کننده:**
فروشندگان و کسب و کارها حتماً در فعالیت‌های تجاری خود، نیازمند دسترسی به شبکه و اطلاعات حساس مشتریان هستند. همچنین ممکن است اجرای برخی کنترل‌های امنیتی بر روی بعضی از تامین کنندگان امکان‌پذیر نباشد. با این حال، برای کاهش خطرات احتمالی، باید کنترل‌های مناسب ازطریق سیاست‌های امنیتی IT و تعهدات قراردادی انجام شود.

**انطباق پذیری:**
در تمامی دستگاه‌های نظارتی باید الزامات امنیتی اجرا شوند.

**سازماندهی امنیت اطلاعات:**
برای برطرف کردن تهدیدات و خطرات موجود در شبکه سازمان‌ها، این مورد از استاندارد ISMS به میان می‌آید. خطراتی نظیر حملات سایبری از مهاجمان خارجی، نقص و اختلال سیستم، تهدیدات داخلی و همچنین از دست رفتن داده‌ها.

**امنیت منابع انسانی:**
در سازمان‌ها سیاست‌ها و کنترل‌هایی مربوط به پرسنل و فعالیت‌ها و خطاهای انسانی وجود دارد. حال برای کاهش خطر تهدیدهای داخل سازمانی و همچنین آموزش نیروی کار برای کاهش صدمات امنیتی، حتماً نیازمند تدوین یک روند ثابت امنیتی خواهید بود.

**مدیریت دارایی‌ها:**
این مولفه از استاندارد ISMS، دارایی‌های سازمانی (چه در داخل سازمان و چه در خارج از آن) و حتی در شبکه IT سازمان، تحت پوشش قرار می‌دهد.

**امنیت اطلاعات و مدیریت حوادث:**
برای حل مسائل و مشکلات مربوط به فناوری اطلاعات، باید از روش‌های شناسایی استفاده شود تا تاثیر آن بر کاربران نهایی (End User) کاهش یابد. همچنین ممکن است راه‌حل‌های پیشرفته فناوری، در محیط‌های پیچیده زیرساخت شبکه، نیاز باشد. به این دلیل که بتوانیم معیارهای حادثه را شناسایی کرده و مسائل احتمالی را کاهش دهیم.

**مدیریت تداوم کسب و کار:**
فرایندهای تجاری ممکن است هرزمان، به دلیلی متوقف شوند. برای به حداقل رساندن آسیب‌های تجاری در حالت ایده‌آل، باید هرگونه شرایط فاجعه‌بار، بلافاصله با مراحل صحیح برطرف شده و بهبود یابند.

**امنیت فیزیکی:**
این دستورالعمل به این منظور ارائه شده است که اقدامات امنیتی را درجهت محافظت از سخت افزارهای فیزیکی، در برابر آسیب‌ها و همچنین محافظت دربرابر ازبین رفتن اطلاعات یا دسترسی‌های غیرمجاز توسعه دهیم. درحالی که بسیاری از سازمان‌ها درسدد فراهم کردن امنیت دیجیتالی برای حفظ اطلاعات در شبکه‌های ابری هستند، تامین امنیت فیزیکی دستگاه‌ها نیز باید در دستور کار آن‌ها قرار گیرد.

## پیاده سازی ISMS

روشهای بی شماری برای دستیابی به اجرای ISMS وجود دارد. متداول ترین روش برای دنبال کردن، فرآیند "Plan Do Check Act" است. خانواده استاندارد ISO 27000 یک راهنمای کامل و جامع برای اجرای ISMS است. ISO / IEC 27001 یک استاندارد امنیتی بین المللی است که جزئیات نیازهای ISMS را بیان می کند. ISO 27001 ، به همراه بهترین دستورالعمل های عملی موجود در ISO 27002 ، به عنوان دو راهنمای عالی برای شروع کار با اجرای ISMS

عمل می کنند. قدرت سیستم مدیریت امنیت اطلاعات (ISMS) بر اساس قدرت ارزیابی ریسک امنیت اطلاعات است که برای هرگونه پیاده سازی، کلیدی است.

مراحل مدل Plan-Do-Check-Act (PCDA) برای بهبود مستمر در فرآیندهای ISMS به قرار زیر می باشد:

- طرح. شناسایی مشکلات و جمع آوری اطلاعات مفید برای ارزیابی ریسک امنیتی. خطمشی‌ها و فرآیندهایی را که می‌توان برای رسیدگی به علل ریشه‌ای مشکل استفاده کرد، تعریف کنید. توسعه روش هایی برای ایجاد بهبود مستمر در قابلیت های مدیریت امنیت اطلاعات.
- انجام دادن. سیاست ها و رویه های امنیتی ابداع شده را اجرا کنید. پیاده سازی از استانداردهای ISO پیروی می کند، اما پیاده سازی واقعی بر اساس منابع در دسترس شرکت شما است.
- بررسی. نظارت بر اثربخشی سیاست‌ها و کنترل‌های ISMS. نتایج ملموس و همچنین جنبه های رفتاری مرتبط با فرآیندهای ISMS را ارزیابی کنید.
- عمل کنید. روی بهبود مستمر تمرکز کنید. نتایج را مستند کنید، دانش را به اشتراک بگذارید و از یک حلقه بازخورد برای رسیدگی به تکرارهای آتی اجرای مدل PCDA سیاست‌ها و کنترل‌های ISMS استفاده کنید

## مراحل طراحی و پیاده سازی ISMS

مراحل طراحی و پیاده سازی سیستم مدیریت امنیت اطلاعات (ISMS) شامل موارد زیر می شود که زمان هر یک از این مراحل با توجه به اهداف یک سازمان، نقطه شروع، روش کار سازمان، میزان مستندات و اطلاعات سازمان و محدوده ای که می خواهید در ISMS خود قرار دهید، متفاوت است.

- **1. ارزیابی و شناخت اولیه (Gap Analysis)**

در فاز ارزیابی و شناخت اولیه، میزان انطباق سازمان با الزامات و کنترل های استاندارد ISO/IEC 27001 مورد بررسی قرار می گیرد. این مرحله، کمک شایانی به تعیین دامنه (scope) پیاده سازی سیستم و فاز طراحی خواهد نمود. فعالیت هایی که در این مرحله اجرا می شود، عبارتند از:

- * شناسایی وضعیت موجود و ارزیابی میزان انطباق سازمان با الزامات و کنترل های استاندارد ISO/IEC 27001
- * مستندسازی و تهیه گزارش از وضعیت موجود
- * تعیین دامنه (scope) پیاده سازی سیستم مدیریت امنیت اطلاعات
- * تهیه و تدوین خط مشی امنیت اطلاعات
- * کمک به سازماندهی و تشکیل کمیته راهبری امنیت در سازمان

- **2. آگاه سازی و آموزش (Awareness & Training)**

در این مرحله، تمامي افراد درگیر در فرآیند پیاده سازی سیستم مدیریت امنیت اطلاعات، آموزش دیده و با مفاهیم و الزامات ISMS آشنا می شوند.

- **3. طراحی ISMS (Planning & Design)**

به منظور موفقیت در پیاده سازیISMS ، می بایست این سیستم را مطابق با الزامات استاندارد و نیازمندی های سازمان طراحی نمود. فعالیت هایی که در این مرحله اجرا می شود، عبارتند از:

- * تهیه لیست دارایی های واقع در دامنه
- * طبقه بندی و ارزش گذاری دارایی های اطلاعاتی
- * تعیین و تدوین متدولوژی ارزیابی مخاطرات
- * تدوین خط مشی ها، دستورالعمل ها و روش های اجرایی مورد نیاز سیستم
- * تدوین طرح تداوم کسب و کار (BCP)
- * تدوین طرح برطرف سازی مخاطرات (RTP)
- * تدوین بیانیه کاربست پذیري (SOA)

- **4. پیاده سازی ISMS (Implementation )**

در این مرحله، کنترل ها، طرح ها و سیاست های امنیتی تهیه شده در فاز قبلی، پیاده سازی می شود.

- **5. ممیزی داخلی و همراهی تا صدور گواهینامه بین المللی (Internal & External Audit)**

پس از پیاده سازی و استقرار کامل سیستم مدیریت امنیت اطلاعات در سازمان، سرممیزان انتخاب شده توسط سازمان، با پیش ممیزی سیستم پیاده سازی شده قبل از ممیزی نهایی، موارد انحرافی و عدم انطباق ها را شناسایی می کنند و با ارایه اقدامات اصلاحی و پیشگیرانه مناسب به منظور رفع عدم انطباق های شناسایی شده، سازمان را تا اخذ گواهینامه بین المللی ISO/IEC 27001 همراهی می نمایند.

### سیستم مدیریت امنیت اطلاعات شامل چه مستنداتی است؟

اما مستندات ISMS شامل چه مواردی هستند و چند نوع از این مستندات باید در یک ساختار درست امنیتی وجود داشته باشد. بر اساس استانداردهای سیستم مدیریت امنیت اطلاعات و ارتباطات، هر سازمان باید مجموعه‌ای از این مستندات را برای خود تدوین کند که شامل موارد زیر است.

- مستند اهداف، راهبردها و سیاست‌های امنیتی فضای تبادل اطلاعات سازمان (Security Policy)
- مستند طرح امنیت فضای تبادل اطلاعات سازمان
- مستند طرح کاهش مخاطرات امنیتی فضای تبادل اطلاعات دستگاه (Risk Assessment)
- مستند برنامه آموزش و آگاهی رسانی امنیتی به پرسنل سازمان (Awareness)
- مستند طرح مقابله با حوادث امنیتی و ترمیم مشکلات و خرابی‌های فضای تبادل اطلاعات دستگاه (Disaster Recovery)

### مزایای پیاده سازی ISMS در یک سازمان

- * امنیت اطلاعات و دارایی های اطلاعاتی
- * حفظ محرمانگی و در دسترس بودن اطلاعات
- * حفظ اطلاعات از بروز تهدیدات، آسیب پذیری ها و مخاطرات در حد امکان
- * آمادگی برای مواجه با حوادثی که امنیت اطلاعات را به مخاطره انداخته اند.
- * ایجاد اطمینان بیشتر برای مدیران، کارکنان، مشتریان و سایر ذینفعان سازمان در مورد امنیت اطلاعات
- * بازگشت هزینه صرف شده برای پیاده سازی ISMS در بلند مدت
- * کاهش هزینه های ترمیم خسارات ناشی از کمبود و نقص موازین امنیتی
- * شناسایی، ارزیابی و حفاظت از دارایی های مهم سازمان همچون: پرسنل کلیدی، دانش پرسنل، اطلاعات سازمان و وجه و اعتبار سازمان
- * اطمینان از تداوم کسب و کار و کاهش صدمات از طریق ایمن ساختن اطلاعات و کاهش تهدیدها
- * امکان رقابت بهتر با سایر سازمان ها

### پیاده سازی سیستم مدیریت امنیت اطلاعات ISMS چه مشکلاتی دارد؟

هر فناوری در کنار مزایای بی شمار، در مراحل نصب و پیاده سازی، مشکلاتی نیز به همراه دارد. در این بخش مشکلات پیاده سازی سیستم مدیریت امنیت اطلاعات را بررسی خواهیم کرد.

- یکی از اصلی‌ترین موانع پیاده سازی استانداردهای سیستم ISMS ، بحث امنیت است. باید به این نکته توجه کنید که امنیت، قبل از آنکه به فناوری تبدیل شود یک فرهنگ است و برای جا افتادن نیاز به زمان زیادی دارد. شما به هیچ وجه نمی‌توانید فرهنگ بومی شده یک سازمان را در یک مرحله فوری به سازمان دیگری وارد کنید.
- هر چند تقریبا غیرممکن است، اما اگر موفق به پیاده سازی سیستم مدیریت امنیت اطلاعات در سازمان شویم و گواهی استاندارد مربوط به آن را نیز در یک مرحله دریافت کنیم، این موارد هرگز «تداوم امنیت» را تضمین نمی‌کند. بنابراین همیشه در استانداردهای بین‌المللی از چرخه دمینگ یا PDCA استفاده می‌شود. که یک چرخه مدور و دائمی برای طراحی، آزمایش و اعمال مجدد عملیات طراحی است. این

چرخه مراحل پیشبرد یک فرآیند را در چهر مرحله طراحی (Plan)، اجرا (Do)، بررسی (Check) و اقدام (Act) تبیین می‌کند. بنابراین می‌توانیم بگوییم این چرخه به شکل مداوم در حرکت است. هر بار تکرار این مراحل به بهبود مستمر سیستم کمک قابل توجهی خواهد کرد.

- به دلیل تداوم ناامنی و تهدید همیشگی اطلاعات سازمان، باید تفکر امنیت و عملیات امن سازی در تمام ابعاد سازمان انجام شده و تداوم داشته باشد. برخی از مدیران در فضای تبادل اطلاعات سازمان، بانک اطلاعات خود را در معرض تهدید و خطر نمی‌بینند و هیچگونه احساس ناامنی ندارند. طبیعی است که با این طرز فکر، حمایت جدی و همه جانبه‌ای هم از پیاده سازی و تداوم استانداردهای مدیریت امنیت اطلاعات انجام نمی‌دهند.
- به این نکته توجه کنید که امنیت چندان قابل احساس نیست. چرا که وقتی یک پروژه امنیتی انجام می‌شود، بعضی مدیران و کارشناسان سازمان احساس می‌کنند هیچ اتفاق خاصی نیفتاده، حتی ممکن است از صرف هزینه برای این پروژه‌ها شکایت کنند. در صورتی که بی توجهی به مدیریت امنیت اطلاعات سازمان، خطرات جبران ناپذیری دارد.